Symmetry, splitting rational places in extensions of function fields and generalization of the Hermitian function field

Vinay Deolalikar [1]

1   Introduction

Let F/K be an algebraic function field in one variable over a finite field of constants K, *i.e.*, F is a finite algebraic extension of $K(x)$ where $x \in F$ is transcendental over K. Let E be a finite separable extension of F. Let $N(E)$ and $g(E)$ denote the number of places of degree one (or *rational* places), and the genus, respectively, of E. Let $[E : F]$ denote the degree of this extension.

In recent years, there has been a spurt of interest in algebraic function fields with many rational places, or, equivalently, curves over finite fields with many rational points. The initial impetus for this interest came from applications to coding theory, wherein, in 1981, Goppa [8] discovered that function fields with many rational places could be used to construct long codes, whose parameters could then be ascertained using the Riemann-Roch theorem. Since then, more applications of such function fields have been discovered [25]. Equally importantly, function fields with many rational places are an interesting mathematical problem in their own right, with connections to several well studied problems in arithmetical algebraic geometry, and have been recognised as such. Consequently, various aspects of such function fields have been studied. Many authors have also written on this subject in the language of curves over finite fields.

One technique to produce function fields with many rational places is to somehow split many rational places of the projective line in an extension, while keeping the rise in genus low. The technique existing in literature that can be used to achieve this uses class field theory and was introduced by Serre [17, 18, 19]. For practical applications of such function fields, however, it is necessary that the constructions be explicit, in that generators and

---

[1] This work was part of the author's Ph.D. thesis and was supervised by the late Prof. Dennis Estes.

equations satisfied by them should be provided. In this paper, we construct infinite families of extensions of the projective line in which all finite rational places split completely, the rise in genus incurred is low, and moreover, the construction is explicit. Furthermore, the constructions described herein work not only over finite fields of square cardinality, but over any non-prime finite field. Our techniques also shed light on why the square cardinality constraint arises in many existing examples.

To these ends, we introduce the notion of "(n, q)-symmetry" which is related to the notion of symmetry in polynomial rings in several indeterminates. For q a prime power and $n \geq 2$, there are n (n, q)-symmetric polynomials, which include trace and norm as the first and n^{th}, respectively. We call these (n, q)-symmetric polynomials $\{s_{n,i}\}_{1 \leq i \leq n}$. These polynomials, among other things, have the property that they map $\mathbb{F}_{q^n}$ into $\mathbb{F}_q$. Using these symmetric polynomials, we then construct two sets (of $n - 1$ families each) of function fields over $\mathbb{F}_{q^n}$, which we name $\{E_i\}_{2 \leq i \leq n}$ and $\{E_{j,Kum}\}_{1 \leq j \leq n-1}$. Function fields belonging to these families are called symmetric function fields. The well known trace-norm function field is merely the special case of the family E_n of our construction. Indeed, we show that it is the *worst* of these families in the sense of N/g ratios. Similarly, many of the existing examples of function fields with many rational places are explained in the language of (n, q)-symmetry, thus unifying several existing examples under one theory.

We show that the N/g ratios for the $n-1$ symmetric families $\{E_i\}$ follow a monotone pattern, namely

$$N(E_2) = N(E_3) = \ldots = N(E_n),$$

$$g(E_2) > g(E_3) > \ldots > g(E_n).$$

We also show that using the techniques described in this paper, we can explicitly construct subcovers of the symmetric function fields, and these also lead to examples with good N/g ratios. Accordingly, we construct two new function fields meeting the Oesterle bounds where one is a subcover of the other.

We also compare our constructions to existing class field theoretic constructions. We show that for identical patterns of ramification groups, symmetric function fields will have better N/g ratios than the corresponding class field theoretic constructions. The function fields that we construct are not maximal - they sit inside of some Ray class fields. Furthermore, while most

of the examples using Ray class fields (example, [10]) have degree greater than the cardinality of the underlying finite field, ours have degrees lesser than that cardinality. This ties in with the approach used by other authors, for example [11], where the minimal function field with a certain property is shown to have the best N/g ratio.

Another point of considerable importance is that in many existing examples of explicitly constructed extensions of function fields where most of the rational places split completely, the genus, and number of rational places, of the resulting function field are usually fairly low. However, for applications to coding theory, one would like to have a large number of rational places in order to build long codes. The function field towers of Garcia and Stichtenoth [5, 6], give us a structure to build long codes, but the problem of finding a basis for the vector spaces of regular functions on them is yet to be solved. The constructions provided in this paper can provide examples of extensions of function fields E/F where all rational places except one split completely, for arbitrarily high degree of extension $[E : F]$, and therefore, for arbitrarily high values of $N(E)$.

Finally, we provide a "generalization" of the Hermitian function field over K where K is an odd degree extension of $\mathbb{F}_q$. For a long time, it has been known that the Hermitian function field has many unique properties, such as its maximality in the Hasse-Weil sense, and its large automorphism group. However there has hitherto not been a satisfactory generalization of this function field to field of nonsquare cardinality. We propose a solution to this problem. We suggest that the trace-norm function field, which has sometimes been implicitly assumed to be the generalization of the Hermitian function field, is not the appropriate generalization. Rather it is the function field E_2 that generalizes the Hermitian.

The paper is organized as follows. In section 2, we introduce the notation used in the rest of the paper. In section 3, we introduce the notion of (n, q)-symmetry and explain how it is related to the notion of symmetry in polynomial rings in several indeterminates. We also derive some elementary properties of (n, q)-symmetric polynomials. In section 4, we construct Artin-Schreier and Kummer extensions of the projective line over $\mathbb{F}_{q^n}$ using (n, q)-symmetric polynomials. We also prove the irreducibility of the defining equations and derive the sequence of ramification groups in the corresponding extensions. These do not follow from basic Artin-Schreier theory since there is no rational place at which the valuation of the 1st to the $(n-1)^{st}$ (n, q)-

3

symmetric polynomials is coprime to the characterisitic. In section 4.1.1, we show how the well-known trace-norm construction is merely a special case of our constructions. In section 5, we compare the N/g ratios for the various symmetric families of function fields, and show that the trace-norm family has the lowest N/g ratio, *i.e.*, all the other families have higher N/g ratios. In section 6, we propose the function field E_2 as the generalization of the Hermitian function field over non-square finite fields. We do this by examining the genus, subgroups of the automorphism groups of the two function fields, and the number of places of degree greater than one.

2 Preliminaries

Throughout this paper, we will use the following notation:

For symmetric polynomials:

$\mathfrak{S}_n$	the symmetric group on n characters
$\mathbf{s}_{n,i}(X)$	the ith elementary symmetric polynomial on n variables
q	a power of a prime p
$\mathbb{F}_l$	the finite field of cardinality l
$s_{n,i}(t)$	the ith (n, q)-elementary symmetric polynomial

For function fields and their symmetric subfields:

K	the finite field of cardinality q^n, where $n > 1$
F/K	an algebraic function field in one variable whose full field of constants is K
F_s	the subfield of F comprising (n, q)-symmetric functions
F_s^ϕ	the subfield of F_s comprising functions whose coefficients are from $\mathbb{F}_q$
E	a finite separable extension of F, $E = F(y)$ where $\varphi(y) = 0$ for some irreducible polynomial $\varphi[T] \in F[T]$

For a generic function field F:

$\mathbb{P}(F)$	the set of places of F
$N(F)$	the number of places of degree one in F
$N_m(F)$	the number of places of degree $m, m > 1$, in F
$g(K)$	the genus of F
P	a generic place in F
v_P	the normalized discrete valuation associated with the place P

4

$\mathcal{O}_P$	the valuation ring of the place P
P'	a generic place lying above P in a finite separable extension of F
$e(P'\|P)$	the ramification index for P' over P
$d(P'\|P)$	the different exponent for P' over P

For the rational function field $K(x)$:

P_α	the place in $K(x)$ that is the unique zero of $x - \alpha$, $\alpha \in K$
P_∞	the place in $K(x)$ that is the unique pole of x

3 Symmetric functions

Let R be an integral domain and $\overline{R}$ its field of fractions. Consider the polynomial ring in n variables over R, given by $R[X] = R[x_1, x_2, \ldots, x_n]$. The symmetric group $\mathfrak{S}_n$ acts in a natural way on this ring by permuting the variables.

Definition 3.1 *A polynomial $\mathbf{f}(X) \in R[X]$ is said to be symmetric if it is fixed under the action of $\mathfrak{S}_n$. If $\mathfrak{S}_n$ is allowed to act on $\overline{R}(X)$ in the natural way, its fixed points will be called symmetric rational functions, or simply, symmetric functions. These form a subfield $\overline{R}(X)_s$ of $\overline{R}(x)$.*

Symmetric functions form a very elegant branch in the study of polynomials with several indeterminates. We recall here one of the classical results on symmetric functions, often known as *The fundamental theorem on symmetric functions*[1].

Theorem 3.2 (The fundamental theorem on symmetric functions)

$$\overline{R}(X)_s = \overline{R}(\mathbf{s}_{n,1}(X), \mathbf{s}_{n,2}(X), \ldots, \mathbf{s}_{n,n}(X))$$

where $\{\mathbf{s}_{n,i}(X)\}_{1 \leq i \leq n}$ are given below:

$$\mathbf{s}_{n,1}(X) \;=\; \sum_{i=1}^{n} x_i,$$

---

[1]A sharper result, called *The fundamental theorem on symmetric polynomials*, says that every symmetric polynomial can be written as a polynomial in the elementary symmetric functions [1].

$$\mathbf{s}_{n,2}(X) \;=\; \sum_{\substack{i<j \\ 1\leq i,j\leq n}} x_i x_j,$$

$$\vdots \qquad \vdots$$

$$\mathbf{s}_{n,n}(X) \;=\; x_1 x_2 \ldots x_n.$$

$\mathbf{s}_{n,i}(X)$ is called the ith elementary symmetric polynomial in n variables.

We would like to apply these notions to the setting of polynomial rings in one variable over finite fields. We start with the following elementary proposition.

Proposition 3.3 *Consider the extension of finite fields given by $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then, the following hold:*

(i) *This is a Galois extension of degree n. The Galois group of this extension, $G = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is cyclic, and is generated by $\phi \in G$, $\phi : \alpha \to \alpha^q$. This generating element is also called the "frobenius" of this extension.*

(ii) *The fixed field of the subgroup of G generated by ϕ^k is $\mathbb{F}_{q^{\gcd(k,n)}}$.*

Definition 3.4 *For the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, we will evaluate the elementary symmetric polynomials (resp. symmetric functions) in $\mathbb{F}_{q^n}(X)$ at $(X) = (t, \phi(t), \ldots, \phi^{n-1}(t)) = (t, t^q, \ldots, t^{q^{n-1}})$. These will be called the (n,q)-elementary symmetric polynomials (resp. (n,q)-symmetric functions). For $\mathbf{f}(X) \in \mathbb{F}_{q^n}(X)$, we will denote $\mathbf{f}(t, t^q, \ldots, t^{q^{n-1}})$ by $f(t)$, or, when the context is clear, by f.*

Thus the (n,q)-elementary symmetric polynomials are the following:

$$s_{n,1}(t) \;=\; \sum_{0\leq i\leq n-1} t^{q^i},$$

$$s_{n,2}(t) \;=\; \sum_{\substack{i<j \\ 0\leq i,j\leq n-1}} t^{q^i} t^{q^j},$$

$$\vdots \qquad \vdots$$

$$s_{n,n}(t) \;=\; t^{1+q+q^2+\ldots+q^{n-1}}.$$

As an example, here are the 5 $(5, q)$-symmetric polynomials.

$s_{5,1}(\text{trace})$	$t^{q^4} + t^{q^3} + t^{q^2} + t^q + t$
$s_{5,2}$	$t^{q^4+q^3} + t^{q^4+q^2} + t^{q^4+q} + t^{q^4+1} + t^{q^3+q^2} + t^{q^3+q}$ $+t^{q^3+1} + t^{q^2+q} + t^{q^2+1} + t^{q+1}$
$s_{5,3}$	$t^{q^4+q^3+q^2} + t^{q^4+q^3+q} + t^{q^4+q^3+1} + t^{q^4+q^2+q} + t^{q^4+q^2+1}$ $+t^{q^4+q+1} + t^{q^3+q^2+q} + t^{q^3+q^2+1} + t^{q^3+q+1} + t^{q^2+q+1}$
$s_{5,4}$	$t^{q^4+q^3+q^2+q} + t^{q^4+q^3+q^2+1} + t^{q^4+q^3+q+1}$ $+t^{q^4+q^2+q+1} + t^{q^3+q^2+q+1}$
$s_{5,5}(\text{norm})$	$t^{q^4+q^3+q^2+q+1}$

We now proceed to give some elementary properties of (n, q)-symmetric polynomials.

Lemma 3.5 *Let $f(t)$ be an (n, q)-symmetric function with coefficients from $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^n}$. Then, we have that $f(\gamma) \in \mathbb{F}_q \cup \infty$.*

Proof. $f(t)$ can be written as a rational function in $\{s_{n,i}(t)\}_{1 \leq i \leq n}$, with coefficients from $\mathbb{F}_q$. By construction, each (n, q)-elementary symmetric polynomial is invariant under the operation of raising to the qth power, modulo $(t^{q^n} - t)$. In other words, each (n, q)-elementary symmetric polynomial, when restricted to $\mathbb{F}_{q^n}$, is invariant under this operation. So are the coefficients, since they are chosen from $\mathbb{F}_q$. The inclusion of infinity in the range comes since γ may be a pole of f. $\qquad \square$

There are n (n, q)-elementary symmetric polynomials. $s_{n,1}$ and $s_{n,n}$ are also known as "trace" and "norm," respectively. In the case of $n = 2$, these are the only (n, q)-elementary symmetric polynomials. For $n \geq 3$, we have a greater choice, which has not been exploited in existing techniques to construct function fields with many rational places. The main thesis of this paper is that these additional polynomials are indeed the more useful ones, as n increases. In particular, we show that a "generalization" of the Hermitian function field can be obtained for $n \geq 3$ by using $s_{n,2}$.

We end this section with some lemmas that will be used later. All of the following are valid for $1 \leq i \leq n$.

Lemma 3.6
$$\frac{s_{n,i}(t)}{s_{n,n}(t)} = s_{n,n-i}\left(\frac{1}{t}\right).$$

Thus, there is a bijection between the set of nonzero roots of $s_{n,i}(t)$ and that of $s_{n,n-i}(t)$. More precisely, $s_{n,i}(\alpha) = 0 \Leftrightarrow s_{n,n-i}(1/\alpha) = 0$, where $\alpha \neq 0$.

Proof. Follows immediately from the relation between $s_{n,i}(t)$ and $s_{n,n-i}(t)$ and observing that the only root of $s_{n,n}(t)$ is zero itself.

Lemma 3.7

$$[s_{n,i}(t)]' = [s_{n-1,i-1}(t)]^q.$$

Proof. The only terms that will contribute to the derivative are those whose exponent is coprime to q, *i.e.*, in which 1 is a summand. There are $\binom{n-1}{i-1}$ such terms and they are all distinct. Moreover, each such term, divided by t, is just the qth power of a term in $s_{n-1,i-1}(t)$. It is easy to see that this correspondence is bijective by noting that there are exactly $\binom{n-1}{i-1}$ terms in $s_{n-1,i-1}(t)$ as well. □

Lemma 3.8 *The roots of $s_{n,i}(t)$ of multiplicity coprime to p lie in $\mathbb{F}_{q^n}$.*

Proof. The proof rests on the observation that

$$
\begin{aligned}
s_{n,i}(t)^q - s_{n,i}(t) &= [t^{q^n} - t][s_{n-1,i-1}(t)]^q, \\
&= [t^{q^n} - t]s_{n,i}(t)', \\
\text{or, } s_{n,i}(t)[s_{n,i}(t)^{q-1} - 1] &= [t^{q^n} - t]s_{n,i}(t)'.
\end{aligned}
$$

Now consider a root α of multiplicity m of $s_{n,i}(t)$ in the algebraic closure of $\mathbb{F}_q$, where $\gcd(m, p) = 1$. This is not a root of the factor $[s_{n,i}(t)^{q-1} - 1]$ and it can only occur to a multiplicity $m - 1$ in $s_{n,i}(t)'$. So it must appear to multiplicity 1 in the factor $[t^{q^n} - t]$ on the RHS. Thus it must lie in $\mathbb{F}_{q^n}$. □

Lemma 3.9 *Every root of $s_{n,i}(t)$ lies in a field $\mathbb{F}_{q^k}$, where $n-i+1 \leq k \leq n$.*

Proof. From Lemma 3.8, we know that if a root of $s_{n,i}(t)$ is not also a root of $s_{n-1,i-1}(t)$, it must lie in $\mathbb{F}_{q^n}$. If, on the other hand, it is a root of $s_{n-1,i-1}(t)$, it either lies in $\mathbb{F}_{q^{n-1}}$ or is a root of $s_{n-2,i-2}$. Now we descend this way till we reach $s_{n-i+1,1}(t)$, all of whose roots lie in $\mathbb{F}_{q^{n-i+1}}$. Notice that $s_{n-i+1,1}(t)$ can have no multiple roots since its derivative is equal to 1. □

Lemma 3.10 *Let α be a root of $s_{n,i}(t)$ of multiplicity $m > 1$. Further let $\gcd(m, p) = \gcd(m - 1, p) = 1$. Then $\alpha \in \mathbb{F}_q$.*

Proof. From Lemma 3.7, we know that the roots of the derivative of $s_{n,i}(t)$ are the same as those of $s_{n-1,i-1}(t)$. From Lemma 3.8, we know that under the hypothesis of the present lemma, the roots in question of $s_{n-1,i-1}(t)$ will lie in $\mathbb{F}_{q^{n-1}}$, while those of $s_{n,i}(t)$ will lie in $\mathbb{F}_{q^n}$. For a common root then, it must be a root of both of these polynomials, and hence must lie in the intersection of both these fields, which is $\mathbb{F}_q$. □

Corollary 3.11 *If p does not divide both $\binom{n}{i}$ and $\binom{n-1}{i-1}$, then there are no non-zero roots of $s_{n,i}(t)$ of multiplicity $m > 1$, such that $\gcd(m,p) = \gcd(m-1, p) = 1$.*

Proof. When restricted to $\mathbb{F}_q$, $s_{n,i}(t) = \binom{n}{i}t^i$, and $s_{n-1,i-1}(t) = \binom{n-1}{i-1}t^{i-1}$. Thus, if the root is non-zero, the only way both these polynomials can be zero is if the characteristic divides both $\binom{n}{i}$ and $\binom{n-1}{i-1}$. □

Lemma 3.12 *$s_{n,1}(t)$ is a permutation polynomial over $\mathbb{F}_{q^m}$ if $\gcd(m,n) = 1$ and p does not divide n.*

Proof. Suppose the pre-image under $s_{n,1}(t)$ of an element comprised of two distinct elements, then, since $s_{n,1}(t)$ is additive, their difference would be its root. But all the roots of $s_{n,1}(t)$ lie in $\mathbb{F}_{q^n}$. If p does not divide n, then none of these lie in $\mathbb{F}_q$. Thus, under these hypotheses, $s_{n,1}(t)$ would not have any roots in $\mathbb{F}_{q^m}$, where $\gcd(m,n) = 1$, and we would get a contradiction. □

Now we wish to use these notions in the setting of an algebraic function field in one variable F/K, where $K = \mathbb{F}_{q^n}$, and F is an algebraic extension of $K(x)$, where x is transcendental over K.

Definition 3.13 *The field of (n,q)-symmetric functions with coefficients in $\mathbb{F}_{q^n}$ will be denoted*

$$F_s = \mathbb{F}_{q^n}\left(s_{n,1}(x), s_{n,2}(x), \ldots, s_{n,n}(x)\right) \subset K(x),$$

and the field of (n,q)-symmetric functions with coefficients in $\mathbb{F}_q$ will be denoted

$$F_s^\phi = \mathbb{F}_q\left(s_{n,1}(x), s_{n,2}(x), \ldots, s_{n,n}(x)\right) \subset K(x),$$

where the superscript ϕ indicates that the values that these functions take on $\mathbb{F}_{q^n}$ are fixed by ϕ. Thus, they lie in $\mathbb{F}_q$, as per Lemma 3.5.

9

4 Symmetric extensions of function fields

Let F and K be as described earlier. Let E be a finite separable extension of F, generated by y, where $\varphi(y) = 0$, for $\varphi(T)$ an irreducible polynomial in $F[T]$.

In this section we will introduce families of extensions of F whose generators satisfy explicit equations involving only (n, q)-symmetric functions. Let y satisfy

$$g(y) = f(x),$$

where $f, g \in F_s^\phi$. If $K = \mathbb{F}_{q^n}$, this implies that in the residue field of a rational place, although the class of x and y will assume values in $\mathbb{F}_{q^n} \cup \infty$, that of $f(x)$ and $g(y)$ will assume values only in $\mathbb{F}_q \cup \infty$. Among the Galois extensions that such equations can produce are the two special cases of extensions of Artin-Schreier and Kummer type. In this paper, we will mainly investigate the case where $f(x)$ is an (n, q)-elementary symmetric polynomial. But the techniques to analyse the case of arbitrary $f \in F_s^\phi$ remain the same.

4.1 Symmetric extensions of Artin-Schreier type

In classical Artin-Schreier extensions, the Galois group is a 1-dimensional vector space over a subfield of the field of constants. We will, however, consider a modified Artin-Schreier extension, where the Galois group is isomorphic to the subgroup of the additive group of $\mathbb{F}_{q^n}$ comprising elements whose trace in $\mathbb{F}_q$ is zero.

Before we proceed to describe such modified Artin-Schreier extensions, we reproduce here some definitions and the relations between the different, ramification groups and the genus in extensions of function fields. References are [12], [16], [22] and [24].

Definition 4.1 *Let F'/F be a finite separable extension of function fields. Then, the different of F'/F, denoted $\mathfrak{D}(F'/F)$, is a divisor in F' given by*

$$\mathfrak{D}(F'/F) = \prod_{P' \in \mathbb{P}(F')} P'^{d(P'|P)},$$

where $d(P'|P)$ is the different exponent of the place P' lying over $P \in \mathbb{P}(F)$. The degree of $\mathfrak{D}(F'/F)$, denoted $\mathrm{degDiff}(F'/F)$, is the degree of this divisor.

Proposition 4.2 (Hurwitz-genus formula) *Let F'/F be a finite separable extension of function fields. Then,*

$$2g(F') - 2 = [F' : F](2g(F) - 2) + \deg\mathrm{Diff}(F'/F).$$

Proposition 4.3 (Transitivity of different) *Let $F \subseteq F' \subseteq F''$, where F''/F' and F'/F are both finite separable extensions. Let $P \subseteq P' \subseteq P''$, where P, P' and P'' are places of F, F' and F'', respectively. Then,*

$$\mathfrak{D}(F''/F) = \mathfrak{D}(F''/F')\mathfrak{D}(F'/F).$$

This yields the following relation between the different exponents

$$d(P''|P) = d(P''|P') + e(P''|P')d(P'|P).$$

Definition 4.4 (Ramification groups) *Let F'/F be a Galois extension of function fields. Let $P \subseteq P'$, where P and P' are places in F and F', respectively. The ith ramification group of $G = \mathrm{Gal}(F'/F)$ relative to P' is $G_i = \{s \in G \mid s(v) \equiv v \bmod P'^{i+1}, \forall v \in \mathcal{O}_{P'}\}$. Then, G_{-1} is the decomposition group, G_0 is the inertia group and G_{-1}/G_0 is $\mathrm{Gal}(K'/K)$, where K and K' are the residue fields of P and P', respectively. Further, G_i is a normal subgroup of G_{-1} as well as G_{i-1}, for $i \geq 0$. G_1 is a p-group and G_0/G_1 is a cylic group of order coprime to p.*

Proposition 4.5 (Hilbert's different formula) *Let F'/F be a Galois extension of function fields. Let $P \subseteq P'$, where P and P' are places in F and F', respectively. Then we have that*

$$d(P'|P) = \sum_{i=0}^{\infty} |G_i| - 1.$$

Proposition 4.6 *Let F''/F be a Galois extension of function fields. Let H be a normal subgroup of $G = \mathrm{Gal}(F''/F)$, and F' be its fixed field. Let P, P' and P'' be places in F, F' and F'', respectively, with $P \subset P' \subset P''$. Then the ith ramification group of $\mathrm{Gal}(F''/F')$ relative to P'' is $G_i \cap H$.*

Now we proceed to describe extensions of modified Artin-Schreier type.

Proposition 4.7 *Let F/K be an algebraic function field, where $K = \mathbb{F}_{q^n}$ is algebraically closed in F. Let $w \in F$ and assume that there exists a place $P \in \mathbb{P}(F)$ such that*

$$v_P(w) = -m, \ m > 0 \ and \ \gcd(m, q) = 1.$$

Then the polynomial $l(T) - w = a_{n-1}T^{q^{n-1}} + a_{n-2}T^{q^{n-2}} + \ldots + a_0 T - w \in F[T]$ is absolutely irreducible. Further, let $l(T)$ split into linear factors over K. Let $E = F(y)$ with

$$a_{n-1}y^{q^{n-1}} + a_{n-2}y^{q^{n-2}} + \ldots + a_0 y = w.$$

Then the following hold:

(i) *E/F is a Galois extension, with degree $[E : F] = q^{n-1}$. $\mathrm{Gal}(E/F) = \{\sigma_\beta : y \to y + \beta\}_{l(\beta)=0}$.*

(ii) *K is algebraically closed in E.*

(iii) *The place P is totally ramified in E. Let the unique place of E that lies above P be P'. Then the different exponent $d(P'|P)$ in the extension E/F is given by*

$$d(P'|P) = (q^{n-1} - 1)(m + 1).$$

(iv) *Let $R \in \mathbb{P}(F)$, and $v_R(w) \geq 0$. Then R is unramified in E.*

(v) *If $a_{n-1} = \ldots = a_0 = 1$, and if $Q \in \mathbb{P}(F)$ is a zero of $w - \gamma$, with $\gamma \in \mathbb{F}_q$. Then Q splits completely in E.*

Proof. For (i) - (iv), pl. refer [23]. For (v), notice that under the hypotheses, the equation $T^{q^{n-1}} + T^{q^{n-2}} + \ldots + T = \gamma$ has q^{n-1} distinct roots in K. $\quad\square$

For many of the extensions that we will describe, there exists no place where the hypothesis of Proposition 4.7 is satisfied, namely, that the valuation of w at the place is negative and coprime to the characteristic. In particular, we need a criterion for determining the irreducibility of the equations that we will need to use. We provide such a criterion in Proposition 4.8 and Corollary 4.10.

Proposition 4.8 *Let V be a finite subgroup of the additive group of $\overline{\mathbb{F}}_p$. Then V is a $\mathbb{F}_p$-vector space. Define $L_V(T) = \prod_{v \in V}(T - v)$. Thus, $L_V(T)$ is a separable $\mathbb{F}_p$-linear polynomial whose degree is the cardinality of V. Now let $h(T, x) = L_V(T) - f(x)$, where $f(x) \in \overline{\mathbb{F}}_p[x]$. Then, $h(T, x) = L_V(T) - f(x)$ is reducible over $\overline{\mathbb{F}}_p[T, x]$ iff there exists a polynomial $g(x) \in \overline{\mathbb{F}}_p[x]$ and a proper additive subgroup W of V such that $f(x) = L_{W'}(g(x))$, where $W' = L_W(V)$.*

Proof. Suppose $h(T, x) = g_1(T, x) \ldots g_n(T, x)$ is a factorization of $h(T, x)$ over $\overline{\mathbb{F}}_p[T, x]$. From Gauss' lemma, and the fact that $h(T, x)$ is monic in T, we see that this is equivalent to a factorization into monic irreducible factors in $\overline{\mathbb{F}}_p(x)[T]$.

Let $F = \overline{\mathbb{F}}_p(x)$ and view $h(T)$ and $g_i(T)$ as polynomials over F. Let $L = F[T]/(g_1(T))$. Then L is a field. Let y be the corresponding root of g_1 in L.

Note that $v \in V$ acts on the roots of $h(T)$ over L via $(T \to T + v)$. Since y is a root of $h(T)$, we see that $h(T)$ splits completely over L, into factors $(T - y - v)$, where $v \in V$.

Also, since $h(T)$ is separable, the factors $g_1(T), \ldots, g_n(T)$ are all distinct. Since the roots of $g_i(T)$ are all conjugate over F, it follows that the action of V on the roots of $h(T)$ must respect the g_i. Thus, the action of V induces an action on the set $\{g_1(T), \ldots, g_n(T)\}$.

Let W be the stabilizer of g_1 in V. Since V is transitive on $\{g_1(T), \ldots, g_n(T)\}$, $|W| = |V/n| = deg(g_1)$. Thus W is isomorphic to the Galois group of $g_1(T)$. It follows that

$$
\begin{aligned}
g_1(T) &= \prod_{w \in W}(T - y - w), \\
&= L_W(T - y), \\
&= L_W(T) - L_W(y).
\end{aligned}
$$

Also note that the factorization of $h(T)$ is nontrivial iff W is a proper subgroup of V.

Now note that the constant term in $g_1(T)$ is $L_W(y)$. Thus $L_W(y) \in F$. In particular, $L_W(y)$ is a polynomial in x with $\overline{\mathbb{F}}_p$ coefficients. It is useful to note that $L_W : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is a homomorphism of additive groups with kernel W. Finally, let $\hat{W}$ be a complement of W in V and let $W' = L_W(V)$. Then

$$
h(T) = \prod_{v \in \hat{W}} \prod_{w \in W}(T - y - v - w),
$$

$$
\begin{aligned}
&= \prod_{v \in \hat{W}} L_W(T - y - v), \\
&= \prod_{v \in \hat{W}} L_W(T) - L_W(y) - L_W(v), \\
&= \prod_{w \in W'} L_W(T) - L_W(y) - w, \\
&= L_{W'}(L_W(T) - L_W(y)), \\
&= L_{W'}(L_W(T)) - L_{W'}(L_W(y)), \\
&= L_V(T) - L_{W'}(L_W(y)).
\end{aligned}
$$

Comparing this to the equation $h(T) = L_V(T) - f$, we see that $f = L_{W'}(L_W(y))$. This proves the proposition. $\qquad\square$

The following observation also follows from the proof of Proposition 4.8. Let $E = F(y)$ be an extension of $F = \overline{\mathbb{F}}_p(x)$ with Galois group V, such that y satisfies the equation $L_V(y) = f(x)$. Let W be a subgroup of index p in V, and let M be its fixed field. Then clearly, $z = L_W(y) \in M$. Let $W' = L_W(V) \cong V/W$. Then we have that

$$
L_{W'}(z) = L_{W'}(L_W(y)) = L_V(y) = f(x).
$$

By noting that the previous equation is of degree p, it follows that $M = F(z)$, where z satisfies the equation

$$
L_{W'}(z) = f(x).
$$

Definition 4.9 *For $f(x) \in \overline{\mathbb{F}}_p[x]$, a coprime term of f is a term with non-zero coefficient in f whose degree is coprime to p. The coprime degree of f is the degree of the coprime term of f having the largest degree.*

Corollary 4.10 *Let $f(x) \in \overline{\mathbb{F}}_p[x]$. Let there be a coprime term in $f(x)$ of degree d, such that there are no terms of degree dp^i for $i > 0$ in $f(x)$. Then $L_V(T) - f(x)$ is irreducible for any subgroup $V \subset \overline{\mathbb{F}}_p$.*

Proof. Suppose $f(x)$ is the image of a linear polynomial $\sum a_n x^{p^n}$. Then the coprime term can only occur in the image of the term $a_0 x$. But then, the images of the coprime term under $a_n x^{p^n}$, for $n > 0$ will have degrees that contradict the hypothesis.

14

EXAMPLE 4.11 *The equation*

$$y^{q^2} + y^q + y = x^{q^2+q} + x^{q^2+1} + x^{q+1}$$

is absolutely irreducible over $\overline{\mathbb{F}}_p$. This follows from Corollary 4.10 by noting that the coprime degree of the RHS is q^2+1, and there are no terms of degree $(q^2+1)p^i$, for $i > 0$.

To state the main theorem of this section which describes a general extension of modified Artin-Schreier type using (n,q)-elementary symmetric functions, we need the following lemma.

Lemma 4.12 *Let $F = K(x)$, where $K = \mathbb{F}_{q^n}, q = p^m, r = m(n-1)$, and $E = F(y)$, where y satisifes the following equation:*

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = f(x),$$

and $f(x) \in F$ is not the image of any element in F under a linear polynomial. Then the following hold:

(i) *E/F is a Galois extension of degree $[E : F] = q^{n-1}$. $\mathrm{Gal}(E/F) = \{\sigma_\beta : y \to y + \beta\}_{s_{n,1}(\beta)=0}$ can be identified with the set of elements in $\mathbb{F}_{q^n}$ whose trace in $\mathbb{F}_q$ is zero by $\sigma_\beta \leftrightarrow \beta$. This gives it the structure of a r-dimensional $\mathbb{F}_p$ vector space.*

(ii) *There exists a tower of subextensions*

$$F = E^0 \subset E^1 \subset \ldots \subset E^r = E,$$

such that for $0 \le i \le r - 1$, $[E^{i+1} : E^i]$ is a Galois extension of degree p.

(iii) *Let $\{b_i\}_{1 \le i \le r}$ be a $\mathbb{F}_p$-basis for $\mathrm{Gal}(E/F)$. Then we can build the tower of subextensions as follows. We set E^j to be the fixed field of the subgroup of the Galois group that corresponds to the $\mathbb{F}_p$-subspace generated by $\{b_1, b_2, \ldots, b_{r-j}\}$. Then, the generators of E^j are $\{y_1, y_2, \ldots, y_j\}$, where $y_1, y_2, \ldots, y_r = y$ satisfy the following relations:*

$$
\begin{aligned}
y^p - B_r^{p-1} y &= y_{r-1}, \\
y_{r-1}^p - B_{r-1}^{p-1} y_{r-1} &= y_{r-2}, \\
\vdots \qquad\qquad &\quad \vdots \\
y_1^p - B_1^{p-1} y_1 &= f(x),
\end{aligned}
$$

15

where,

$$\begin{aligned}
\beta_{r,j} &= b_{r-j+1}, & B_r &= \beta_{r,r}, \\
\beta_{r-1,j} &= \beta_{r,j}^p - B_r^{p-1}\beta_{r,j}, & B_{r-1} &= \beta_{r-1,r-1}, \\
&\vdots \qquad \vdots & &\vdots \\
\beta_{1,j} &= \beta_{2,j}^p - B_2^{p-1}\beta_{2,j}, & B_1 &= \beta_{1,1}.
\end{aligned}$$

Proof. For (i) refer Proposition 4.7 and Proposition 4.8. For (ii), note that since $\mathrm{Gal}(E/F)$ is an elementary Abelian group of exponent p, we can always find a normal series $\mathrm{Gal}(E/K) = G^0 \rhd G^1 \rhd \ldots \rhd G^r = 1$ such that $|G^{i+1}/G^i| = p$. Now the existence of a tower $E^0 \subset E^1 \subset \ldots \subset E^r$, with E^{j+1}/E^j Galois of degree p is guaranteed by the Fundamental Theorem of Galois Theory by setting E^i to be the fixed field of G^i. Alternately, we can get a constructive proof for (ii) from the proof for (iii), which follows.

For (iii), we set G^{r-1} to be the $\mathbb{F}_p$-span of b_1 and E^{r-1} to be its fixed field. Then, the automorphisms of E^r/E^{r-1} are given by $y \to y + ab_1$, with $a \in \mathbb{F}_p$. Thus we have that

$$\prod_{a \in \mathbb{F}_p} y - ab_1 = b_1^p \prod_{a \in \mathbb{F}_p} \frac{y}{b_1} - a = y^p - b_1^{p-1}y = y_{r-1}.$$

Now, we set G^{r-2} to be the $\mathbb{F}_p$-span of $\{b_1, b_2\}$, and iterate this procedure for E^{r-1}/E^{r-2}, keeping in mind that the automorphism of E/F given by $y \to y + b_2$, when pulled down to an automorphism of E^{r-1}/E^{r-2}, is given by $y_{r-1} \to y_{r-1} + b_2^p - b_1^{p-1}b_2$. By similarly setting $G^{r-j}, j \geq 2$ to be the $\mathbb{F}_p$-span of $\{b_1, b_2, \ldots, b_j\}$, and pulling down the appropriate automorphisms of E/F to those of E^{r-j+1}/E^{r-j} we get the other defining equations. The observation made after the proof of Proposition 4.8 completes the proof. $\square$

Corollary 4.13 *Let E, F, K be as in Lemma 4.12. Then, every subextension E^1 of E which has degree p over F is of the form $F(z)$, where z satisfies an equation*

$$z^p - Az = f(x),$$

where $A \in \mathbb{F}_{q^n}$.

It is useful to note that since E^1 is the fixed field of a subgroup of $\mathrm{Gal}(E/F)$ of index p, we can obtain a basis for $\mathrm{Gal}(E/F)$ by adding one more element to a basis for this subgroup.

We are now in a position to state our main theorem for this section.

Theorem 4.14 *Let $F = K(x)$ where $K = \mathbb{F}_{q^n}$, $q = p^m$ and $r = m(n-1)$. Consider the family of extensions $E_i = F(y)$, $2 \leq i \leq n$, where y satisfies the equation*

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = s_{n,i}(x). \tag{1}$$

Then the following hold:

(i) *E_i/F is a Galois extension, with degree $[E_i : F] = q^{n-1}$. $\mathrm{Gal}(E_i/F) = \{\sigma_\beta : y \to y + \beta\}_{s_{n,1}(\beta)=0}$.*

(ii) *The only place of F that is ramified in E_i is the unique pole P_∞ of x. Furthermore, P_∞ is totally ramified in E_i. Let P'_∞ denote the unique place of $\mathbb{P}(E_i)$ that lies above P_∞.*

(iii) *Let m_i denote the coprime degree of $s_{n,i}(x)$. We have that*

$$m_i = q^{n-1} + q^{n-2} + \ldots + q^{n-i+1} + 1.$$

The filtration of ramification groups relative to P'_∞ is as follows:

$$\mathrm{Gal}(E_i/F) = G_0 = G_1 = \ldots = G_{m_i+1},$$

$$G_{m_i+2} = \{0\}.$$

(iv) *The different exponent $d(P'_\infty|P_\infty)$ is given by*

$$d(P_\infty|P'_\infty) = (q^{n-1} - 1)(m_i + 1).$$

(v) *The genus of E_i is given by*

$$g(E_i) = \frac{(q^{n-1} - 1)(m_i - 1)}{2}.$$

(vi) *All other rational places of F split completely in E_i giving*

$$N(E_i) = q^{2n-1} + 1.$$

Thus, the number of rational places is independent of the choice of (n,q)-elementary symmetric polynomial of x.

Proof. (i) follows from Corollary 4.10 by observing that p times the coprime degree of $s_{n,i}(x)$ is greater than its degree. Let $G = \mathrm{Gal}(E_i/F)$. To determine the sequence of ramification groups of G relative to P'_∞, we will use the function i_G defined on the elements of the G as follows:

$$i_G(s) \geq k+1 \Leftrightarrow s \in G_k.$$

For every subgroup H of G, define $(G/H)_k$ to be the kth ramification group of the fixed field of H, relative to its unique place lying above P_∞. Then, define the function $i_{G/H}$ on the elements of G/H as follows:

$$i_{G/H}(\overline{s}) \geq k+1 \Leftrightarrow \overline{s} \in (G/H)_k.$$

Note that for all subgroups H of index p in G, we know that

$$i_{G/H}(\overline{s}) \;=\; \begin{cases} \infty & \text{if } \overline{s} = 0, \\ m_i + 2 & \text{else.} \end{cases}$$

We claim that if K is any proper subgroup of G then the average of the values of the function $i_{G/K}$ on the non-zero elements of G/K,

$$\mathrm{avg}_{s \in G/K, s \neq 0} i_{G/K}(s) = m_i + 2.$$

To see this, suppose that $|G/K| = p^l$. Consider the subgroups H such that $K \subset H \subset G$, with $[G:H] = p$. These are in $1:1$ correspondence with the subgroups of index p in G/K, which number $\frac{p^l-1}{p-1}$. A non-zero element $s \in G/K$ is contained in exactly $\frac{p^{l-1}-1}{p-1}$ of these. Now, from [16], Ch. IV, Proposition 3, we get

$$i_{G/H}(\overline{s}) = \frac{1}{p^{l-1}} \sum_{s \to \overline{s}} i_{G/K}(s).$$

Since each non-zero $s \in G/K$ is nontrivial in exactly p^{l-1} of the G/H, so that summing over all non-zero $s \in G/K$, we get

$$\sum_{\substack{K \subset H \subset G, [G:H]=p \\ \overline{s} \in G/H, \overline{s} \neq 0}} i_{G/H}(\overline{s}) = \sum_{s \in G/K} i_{G/K}(s).$$

But as noted previously, each $i_{G/H}(\overline{s}) = m_i + 2$. Since each side in the previous equation has the same number of terms, the average of the RHS $=$ average of the LHS $= m_i + 2$. This proves the claim.

18

It now follows that $i_G(s) = m_i + 2$ for all non-zero $s \in G$. For suppose not. Then there must exist $s \in G$ such that $i_G(s) > m_i + 2$. Since i_G is constant on cyclic subgroups, we see that $\langle s \rangle \neq G$. But then the average on $G/\langle s \rangle$ will be less than $m_i + 2$, giving a contradiction.

(iv) now follows from Hilbert's different formula. (v) is a straightforward application of the Hurwitz-genus formula. (vi) follows from Proposition 4.7. We obtain the number of rational places in E_i as follows. Each of the q^n finite places in F splits completely in E_i, giving $(q^n)(q^{n-1}) = q^{2n-1}$ rational places in E_i. Also, P_∞ ramifies totally in E_i, giving a sum total of $q^{2n-1} + 1$ rational places in E_i. $\square$

EXAMPLE 4.15 (n=3, i=2) Let $F = K(x)$, where $K = \mathbb{F}_{q^3}$. Let $E = F(y)$ where y satisfies the equation

$$y^{q^2} + y^q + y = x^{q^2+q} + x^{q^2+1} + x^{q+1}.$$

All rational places of F, except P_∞, split completely in E, giving a total of $(q^3)(q^2) = q^5$ rational places. Also, P_∞ ramifies totally in E giving one rational place. Thus, $N(E) = q^5 + 1$ rational places. The genus $g(E) = \frac{(q^2-1)(q^2)}{2}$. In a later section we will see that this extension attains the Oesterle lower bound on genus for $q = 2$, i.e., over $\mathbb{F}_{q^3} = \mathbb{F}_8$.

EXAMPLE 4.16 (n=3, i=2) In this example, we discuss a subfield of the Example 4.15. Let E, F, K all be as in Example 4.15. Then consider the extension E^1/F where $E^1 = F(y_1)$, and y_1 satisfies the equation

$$y_1^q + (1 + b^{q^2-q})y_1 = x^{q^2+q} + x^{q^2+1} + x^{q+1},$$

where $b(\neq 0) \in K$ is an element whose trace in $\mathbb{F}_q$ is zero. Then E^1 is a subfield of E and $E = E^1(y)$, with y satisfying

$$y^q - b^{q-1}y = y_1.$$

P_∞ is totally ramified in E^1 and all other rational places of F split completely in E^1 (This is clear since E^1 is a subfield of E, in which these statements are true). Let P_∞^1 be the unique place of E^1 lying above P_∞. Then we have that $d(P_\infty^1|P) = (q-1)(q^2+2)$ and $g(E^1) = \frac{(q-1)(q^2)}{2}$. Also, $N(E^1) = q^4 + 1$. E^1 also attains the Oesterle lower bound on genus for $q = 2$.

EXAMPLE 4.17 (n=4, i=3) Let $F = K(x)$, where $K = \mathbb{F}_{q^4}$. Let $E = F(y)$ where y satisfies the equation

$$y^{q^3} + y^{q^2} + y^q + y = x^{q^3+q^2+q} + x^{q^3+q^2+1} + x^{q^3+q+1} + x^{q^2+q+1}.$$

All rational places of F, except P_∞, split completely in E. P_∞ ramifies totally in E. This gives us $N(E) = q^7 + 1$. The genus $g(E) = \frac{(q^3-1)(q^3+q^2)}{2}$.

Definition 4.18 *A function field F/K, where $K = \mathbb{F}_{q^n}$ is said to be median if $N(F) = q^n + 1$. Thus, the number of its rational places is exactly in the middle of the range allowed by the Hasse-Weil bound.*

Proposition 4.19 *Let $F = K(x)$, where $K = \mathbb{F}_{q^m}$, $\gcd(m, n) = \gcd(p, n) = 1$. Let $E_i = F(y)$ where y satisfies the equation*

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = s_{n,i}(x).$$

Then E_i is median[2]. It retains this property if we replace $s_{n,i}(x)$ with any other polynomial such that the resulting equation is irreducible.

Proof. From Lemma 3.12, we know that under the hypothesis, $y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y$ simply permutes the elements of $\mathbb{F}_{q^m}$. Then, for every value that x can take in $\mathbb{F}_{q^m}$, we have exactly one solution for y. $\square$

EXAMPLE 4.20 The following are the 4 symmetric Artin-Schreier extensions of $\mathbb{F}_{q^5}(x)$. Notice that E_5 is the familiar trace-norm construction. All of these have the same number of rational points, and the genus increases in the order

$$g(E_2) < g(E_3) < g(E_4) < g(E_5).$$

---

[2]Function fields which are median over infinitely many extensions of their field of constants ($\mathbb{F}_q$ in our case) are called *exceptional*. There is a rich theory to such function fields. For instance, it is known [3] that the roots of their zeta-function occur in cliques as roots of unity times each other.

In other words, the trace-norm has the worst (lowest) N/g ratio.

E_2	$y^{q^4} + y^{q^3} + y^{q^2} + y^q + 1 = x^{q^4+q^3} + x^{q^4+q^2} + x^{q^4+q} + x^{q^4+1} +$ $x^{q^3+q^2} + x^{q^3+q} + x^{q^3+1} + x^{q^2+q} + x^{q^2+1} + x^{q+1}$
E_3	$y^{q^4} + y^{q^3} + y^{q^2} + y^q + 1 = x^{q^4+q^3+q^2} + x^{q^4+q^3+q} + x^{q^4+q^3+1} + x^{q^4+q^2+q}$ $+x^{q^4+q^2+1} + x^{q^4+q+1} + x^{q^3+q^2+q} + x^{q^3+q^2+1} + x^{q^3+q+1} + x^{q^2+q+1}$
E_4	$y^{q^4} + y^{q^3} + y^{q^2} + y^q + 1 = x^{q^4+q^3+q^2+q} + x^{q^4+q^3+q^2+1}$ $+x^{q^4+q^3+q+1} + x^{q^4+q^2+q+1} + x^{q^3+q^2+q+1}$
E_5	(trace-norm)$y^{q^4} + y^{q^3} + y^{q^2} + y^q + 1 = x^{q^4+q^3+q^2+q+1}$

4.1.1 Special case: $i = n$ (trace-norm)

It has been known that in extensions of the form E/F where $E = F(y)$ with

$$s_{n,1}(y) = s_{n,n}(x),$$

all the rational places of F, except P_∞, split completely, yielding many rational places in E. Extensions of this form have been referred to as "trace-norm" extensions. However, we will treat this type of extension as a special case of the generalized symmetric extensions of Theorem 4.14. In the notation of Theorem 4.14, the trace-norm extension is E_n.

The most famous example of a trace-norm construction is the Hermitian function field with full field of constants $\mathbb{F}_{q^2}$ (*i.e.*, the case $n = 2$), where the trace and norm are taken down to $\mathbb{F}_q$. This is a maximal function field in the Hasse-Weil sense. Whenever $q \neq p$, we may take the trace and norm down to a smaller subfield of $\mathbb{F}_q$. All three - the degree of the extension, the number of rational places, and the genus - for such a construction increase as we take traces and norms to smaller subfields. The maximum for each of these is attained when we take the trace and norm down to the prime field $\mathbb{F}_p$.

For a function field over K, we may then construct trace-norm extensions by taking these into any subfield of K. In the language of $(n/m, q^m)$-elementary symmetric polynomials, the most general form of the trace-norm extension is given by

$$s_{\frac{n}{m},1}(y) = s_{\frac{n}{m},\frac{n}{m}}(x),$$

where the trace and norm are being taken in the subfield $\mathbb{F}_{q^m}$. Now we would like to see how the ratio N/g in such extensions varies as we vary m from

1 to the value of the greatest proper divisor of n. In other words, we would like to see how this ratio varies as we change the subfield of K in which we take the trace and norm.

Lemma 4.21 *Let $F = K(x)$ where $K = \mathbb{F}_{q^n}$. Let $m \neq n, m|n$ and $\frac{n}{m} = r$. Let $E = F(y)$, where y satisfies the equation*

$$y^{q^{m(r-1)}} + y^{q^{m(r-2)}} + \ldots + y = x^{q^{m(r-1)}+\ldots+q^m+1}. \tag{2}$$

Thus, the trace and norm are being taken to the field $\mathbb{F}_{q^m}$. Then the following holds:

(i) *The ratio N/g, of the number of rational places to genus, decreases with decreasing m.*

(ii) *If $n \equiv 0 \bmod 2$, the maximum value of N/g for the extension of this type is obtained by taking trace and norm down to the field of cardinality $q^{\frac{n}{2}}$.*

Proof. In the general case, $N(E) = q^{2n-m} + 1$, and $g(E) = \frac{q^m(q^{n-m}-1)^2}{2(q^m-1)}$. Thus,

$$\frac{N(E)}{2g(E)} = \frac{(q^m - 1)(q^m + q^{2n})}{(q^n - q^m)^2}.$$

The numerator increases with increasing m while the denominator decreases with increasing m. The result follows. $\qquad \square$
Note: Lemma 4.21, (ii) is the case of the Hermitian function field.

Corollary 4.22 *For extensions of the form given by Lemma 4.21, the lowest value of the ratio N/g is reached when we take norms and traces down to $\mathbb{F}_p$.*

There are other extensions of function fields using trace and norm, and one of them is given below.

EXAMPLE 4.23 Let $F = K(x)$, where $K = \mathbb{F}_{q^2}$. Let $E = F(y)$ with

$$y^q + y = \frac{x^{q+1}}{x^q + x}.$$

22

This is the function field at the second step of the tower of function fields attaining the Drinfeld-Vladut bound from [6]. The only places of $\mathbb{P}(F)$ that are ramified in E are P_∞ and $\{P_\alpha\}_{s_{2,1}(\alpha)=0,\alpha\neq 0}$. These are totally ramified, each with different exponent $2(q-1)$. All other rational places split completely. Thus we have that $N(E) = q^3 - q^2 + 2q$ and $g(E) = (q-1)^2$.

Lemma 4.24 *The extension E_n described in Theorem 4.14 attains the Hasse-Weil bound for $n = 2$, for all values of q. For $n > 2$, it does not attain the Hasse-Weil bound for any value of q.*

Proof. Observe that for $n > 2$,

$$\frac{q(q^{n-1}-1)^2}{2(q-1)} > \frac{q^{\frac{n}{2}}(q^{\frac{n}{2}}-1)}{2}.$$

The lemma then follows from a well-known result that says that a function field over $\mathbb{F}_l$ cannot attain the Hasse-Weil bound for genus $g > \frac{\sqrt{l}(\sqrt{l}-1)}{2}$, cf. [22], Ch. V.3.3. $\qquad\square$

4.2   Symmetric extensions of Kummer type

We now study extensions whose Galois group is a subgroup of the multiplicative group K^*. For this we will need that the field contain a primitive j^{th} root of unity ξ_j for some j coprime to p. In particular we know that K contains ξ_j for $j = \frac{q^n-1}{q-1}$.

Theorem 4.25 *Let $F = K(x)$ where $K = \mathbb{F}_{q^n}$. Let $E_{i,Kum} = F(y)$, $1 \leq i \leq n-1$, where y satisfies the equation*

$$y^{\frac{q^n-1}{q-1}} = s_{n,i}(x). \tag{3}$$

Then the following hold:

(i) *$E_{i,Kum}/F$ is a cyclic Galois extension, with degree $[E_{i,Kum} : F] = \frac{q^n-1}{q-1}$. $\mathrm{Gal}(E_{i,Kum}/F) = \{\sigma_j : y \to y\xi^k\}_{1 \leq k \leq \frac{q^n-1}{q-1}}$.*

(ii) *The only places of F that are ramified in $E_{i,Kum}$ are P_∞ and $\{P_\alpha\}_{s_{n,i}(\alpha)=0}$. Let $v_P = v_P(s_{n,i}(x))$. Define $r_\alpha = \gcd([E_{i,Kum} : F], v_{P_\alpha}) > 0$ and $r_\infty = \gcd([E_{i,Kum} : F], v_{P_\infty}) > 0$. Then we have that*

$$e(P'_\alpha|P_\alpha) = \frac{[E_{i,Kum} : F]}{r_\alpha},$$

$$e(P'_\infty|P_\infty) = \frac{[E_{i,Kum} : F]}{r_\infty}.$$

Since the extension is tame, the different exponents are given by

$$d(P'|P) = e(P'|P) - 1, \ \forall P' \in \mathbb{P}(E).$$

Also, $v_{P_0}(s_{n,i}(x)) = \frac{q^i-1}{q-1}$ and $v_{P_\infty}(s_{n,i}(x)) = q^{n-i}(\frac{q^i-1}{q-1})$.

(iii) *All other rational places of $\mathbb{F}_{q^n}(x)$ split completely in $E_{i,Kum}$.*

Proof. The proofs for (i) and (ii) will need standard results on Kummer extensions, cf. [22], Ch. III.7.3. Also note that $r_\alpha, r_\infty < \frac{q^n-1}{q-1}$. For (iii) we note that from Lemma 3.5, $s_{n,i}(\gamma) \in \mathbb{F}_q, \forall \gamma \in \mathbb{F}_{q^n}$, and therefore, it has $\frac{q^n-1}{q-1}$ pre-images under the norm map. $\square$

Lemma 4.26

$$E_{i,Kum} \cong E_{n-i,Kum}.$$

Proof. By making the substitution $y = xy'$, and then using Lemma 3.6. $\square$
  This immediately leads to the following corollary.

Corollary 4.27 *The extensions $E_{1,Kum}$ and $E_{n-1,Kum}$ of Theorem 4.25 are both isomorphic to the trace-norm extension E_n of Theorem 4.14.*

EXAMPLE 4.28 The following are the symmetric Kummer extensions of $\mathbb{F}_{q^5}(x)$. $E_{1,Kum}$ is again the trace-norm extension.

$E_{1,Kum}$	(trace-norm)$y^{q^4+q^3+q^2+q+1} = x^{q^4} + x^{q^3} + x^{q^2} + x^q + 1$
$E_{2,Kum}$	$y^{q^4+q^3+q^2+q+1} = x^{q^4+q^3} + x^{q^4+q^2} + x^{q^4+q} + x^{q^4+1}+$ $x^{q^3+q^2} + x^{q^3+q} + x^{q^3+1} + x^{q^2+q} + x^{q^2+1} + x^{q+1}$
$E_{3,Kum}$	$y^{q^4+q^3+q^2+q+1} = x^{q^4+q^3+q^2} + x^{q^4+q^3+q} + x^{q^4+q^3+1} + x^{q^4+q^2+q}$ $+x^{q^4+q^2+1} + x^{q^4+q+1} + x^{q^3+q^2+q} + x^{q^3+q^2+1} + x^{q^3+q+1} + x^{q^2+q+1}$
$E_{4,Kum}$	$y^{q^4+q^3+q^2+q+1} = x^{q^4+q^3+q^2+q} + x^{q^4+q^3+q^2+1} + x^{q^4+q^3+q+1}$ $+x^{q^4+q^2+q+1} + x^{q^3+q^2+q+1}$

EXAMPLE 4.29 (n=3, i=2) Let $F = K(x)$, where $K = \mathbb{F}_8$. Let $E = F(y)$ where y satisifes the equation

$$y^7 = x^6 + x^5 + x^3 \ (= s_{3,2}(x)).$$

$s_{3,2}(x)$ has three distinct zeros, other than 0 itself, which has multiplicity three. $N(E) = 33$ and $g(E) = 9$. From Corollary 4.27, we can see why these are the same values as the corresponding trace-norm extension.

There are other examples of Kummer extensions using (n, q)-elementary symmetric polynomials alone. An example from [7] is given below.

EXAMPLE 4.30 Let $F = \mathbb{F}_q(x)$, $q = p^e, e > 1, m = \frac{q-1}{p-1}$, and let $E = F(y)$ with

$$y^m = (1 + x)^m + 1.$$

Here m rational places in $\mathbb{P}(F)$ ramify, while all others split completely in E. Notice that P_∞ splits completely in this extension, unlike the extensions of Theorem 4.25. This construction, when iterated, gives an asymptotically good tower [7].

5 Number of rational places versus genus

In order to arrive at the Oesterle lower bound on genus g of a function field for a specified field of constants $\mathbb{F}_q$ and specified number of rational places $N = L + 1$, one must go through an algorithm of sorts, that is given below [15].

(1) Let m be the unique integer for which

$$\sqrt{q}^m < L \le \sqrt{q}^{m+1}.$$

(2) Define

$$u = \frac{\sqrt{q}^{m+1} - L}{L\sqrt{q} - \sqrt{q}^m} \in [0, 1).$$

(3) Let θ_0 be the unique solution of the trigonometric equation

$$\cos\frac{m+1}{2}\theta + u\cos\frac{m-1}{2}\theta = 0$$

in the interval $[\frac{\pi}{m+1}, \frac{\pi}{m}]$.

(4) Then we have that

$$g \geq \frac{(L-1)\sqrt{q}\cos\theta_0 + q - L}{q+1-2\sqrt{q}\cos\theta_0}.$$

EXAMPLE 5.1 If $q = 8$ and $N = 17$, then we have that $m = 2$, $u = 0.1779$ and $\theta_0 = 1.1472$ yielding $g \geq 1.414$. Thus for a function field over $\mathbb{F}_8$ to have 17 rational places, it must have genus at least 2.

EXAMPLE 5.2 If $q = 8$, and $N = 33$, then we have that $m = 3$, $u = 0.47$ and $\theta_0 = 0.88735$, yielding $g \geq 5.779$. Thus for a function field over $\mathbb{F}_8$ to have 33 rational places, it must have genus at least 6.

EXAMPLE 5.3 If $q = 16$, and $N = 129$, then we have that $m = 3, u = 0.2857$ and $\theta_0 = 0.87752$, yielding $g \geq 17.88$. Thus for a function field over $\mathbb{F}_{16}$ to have 129 rational places, it must have genus at least 18.

EXAMPLE 5.4 If $q = 27$, and $N = 244$, then we have that $m = 3, u = 0.433$ and $\theta_0 = 0.90754$, yielding $g \geq 25.16$. Thus for a function field over $\mathbb{F}_{27}$ to have 244 rational places, it must have genus at least 26.

Now we investigate the performance of symmetric function fields with respect to the known (Hasse-Weil, Oesterle) bounds on the number of rational places.

Theorem 4.14 describes, for a specific value of n, $n-1$ different symmetric extensions of the rational function field corresponding to $i = 2, 3, \ldots, n$. The case of $i = n$ is the trace-norm extension. We now compare these $n-1$ different extensions for various values of q.

n	q	$N(E)$	$g_n(E)$	$g_{n-1}(E)$	$g_{n-2}(E)$	$g_{n-3}(E)$	Oesterle
3	2	(17)		(2)*			2*
3	2	33	9	6*			6*
3	4	1025	150	120			74
3	8	32769	2268	2016			903
3	3	244	48	36			26
3	9	59050	3600	3240			1374
3	5	3126	360	300			167
3	7	16808	1344	1176			560
3	11	161052	7920	7620			2808
4	2	129	49	42	28		18
4	4	16385	2646	2560	2016		667
4	3	2188	507	468	351		152
4	5	78126	9610	9300	7750		2071
5	2	513	225	210	180	120	57

Table 1: Number of rational points and genus for some members of the families of symmetric function fields. The entry $g_j(E)$ denotes the genus of the extension described by Theorem 4.14 obtained for $i = j$. Note that $g_n(E)$ is the genus of the trace-norm extension. * indicates that the function field attains the Oesterle bound, and parentheses indicate a subfield of the symmetric function field.

As Theorem 4.14 tells us, the extension E_2 always has the lowest genus, while the extension E_n (the trace-norm extension) has the highest genus. In other words, for purposes of the ratio of N/g, the trace-norm extension is actually the *worst* of the symmetric extensions, while the extension that uses the second (n, q)-symmetric polynomial is the *best*.

We now look more closely at the case of $n = 3$, $i = 2$, since this contains a maximal member in the the Oesterle sense. Specifically, we provide a uniformizing parameter at the place P'_∞.

EXAMPLE 5.5 Let $F = K(x)$, where $K = \mathbb{F}_{q^3}$. Let $E = F(y)$ where y satisfies the equation

$$y^{q^2} + y^q + y \; = \; x^{q^2+q} + x^{q^2+1} + x^{q+1}.$$

Except for P_∞, which is totally ramified, all other rational places in F split completely in E, giving a total of $q^5 + 1$ rational places. A uniformizing parameter for P'_∞ can be obtained as follows. First we make the substitutions $x = X/Z$ and $y = Y/Z$ to get the following homogeneous equation:

$$Y^{q^2}Z^q + Y^q Z^{q^2} + YZ^{q^2+q-1} = X^{q^2+q} + X^{q^2+1}Z^{q-1} + X^{q+1}Z^{q^2-1},$$

where, we look at $Y = 1, Z = 0$ (*i.e.*, P'_∞), and we get

$$Z^q + Z^{q^2} + Z^{q^2+q-1} = X^{q^2+q} + X^{q^2+1}Z^{q-1} + X^{q+1}Z^{q^2-1}.$$

Note that the valuations for x, y, X, Y and Z at P'_∞ are $-q^2, -(q^2+q), q, 0$ and $q^2 + q$, respectively. Now, we expand Z in a power series in X:

$$Z = X^{q+1} + X^{2q} + \frac{X^{2q+1}}{\pi},$$

where π has valuation of the qth root of X, *i.e.*, it is a uniformizing parameter for P'_∞. Thus we get a uniformizing parameter π for P'_∞ given by:

$$\pi = \frac{X^{2q+1}}{Z - X^{q+1} + X^{2q}} = \frac{x^{2q+1}}{y^{2q} - x^{q+1}y^q - x^{2q}y}.$$

Now, let $\sigma_\beta \in \mathrm{Gal}(E/F)$ be such that $\sigma_\beta : y \to y + \beta$, where β is a non-zero element of $\mathbb{F}_{q^3}$ whose trace in $\mathbb{F}_q$ is zero. Then,

$$\sigma_\beta(\pi) - \pi = \frac{x^{2q+1}[\beta^{2q} + 2\beta^q y^q - \beta^q x^{q+1} - \beta x^{2q}]}{[(y+\beta)^{2q} - x^{q+1}(y+\beta)^q - x^{2q}(y+\beta)][y^{2q} - x^{q+1}y^q - x^{2q}y]}.$$

By noting that the valuation of both the terms in the denominator is the same, since they are conjugates, and then observing that the term in the numerator whose valuation will dominate is the last one, we get the valuation of $\sigma_\beta(\pi) - \pi$, which is independent of the choice of β:

$$v_{P'_\infty}(\sigma_\beta(\pi) - \pi) = q^2 + 2.$$

This again gives us the sequence of ramification groups:

$$G_0 = G_1 = \ldots = G_{q^2+1},$$

$$G_{q^2+2} = \{0\}.$$

Thus the different exponent and the degree of the different for the extension E/F are

$$d(P'_\infty|P_\infty) = \mathrm{degDiff}(E/F) = (q^2 + 2)(q^2 - 1).$$

This agrees with the results given in Theorem 4.14.

We now wish to compare extensions of the rational function field having the typical (to our family of extensions) jumps in the sequence of ramification groups relative to the unique ramified place but having different degrees as extensions of the rational function field.

Theorem 5.6 *Let $F = K(x)$ and $K = \mathbb{F}_q$. Let E/F be an extension of function fields of degree d, where the sequence of ramification groups relative to the unique ramified place is of the form*

$$G_0 = G_1 = \ldots = G_k,$$

$$G_{k+1} = \{0\}.$$

Further let all other places in F split completely in E. Then the ratio of N/g for E decreases with increasing d.

Proof. We have that

$$
\begin{aligned}
N &= dq + 1, \\
2g &= 2 - 2d + (d-1)(k+1) = (d-1)(k-1), \\
\frac{N}{2g} &= \frac{dq + 1}{(d-1)(k-1)}.
\end{aligned}
$$

Then differentiating w.r.t d, we get that

$$\left[\frac{N}{2g}\right]' = \frac{(q+1)(1-k)}{[(d-1)(k-1)]^2}.$$

Now notice that $k \geq 2$ for $g(E) > 0$. But in that case the numerator is always nonpositive. Hence the result. $\square$

Thus, we get higher N/g ratios by looking at subfields that have identical jumps in their sequence of ramification groups. The smaller the subfield, the higher is the N/g ratio. In a sense, the rational function field is the limiting case of this behaviour, with $N/g = \infty$.

Thus ray class field extensions, which are maximal Abelian extensions with a certain property, have lower N/g ratios than other Abelian extensions having identical jumps in their sequence of ramification groups.

EXAMPLE 5.7 Consider the extension of Example 5.5. Let $q = 2$ and $G = \mathrm{Gal}(E/F)$. Then the filtration of ramification groups at P'_∞ is $G = G_0 = G_1 = \ldots = G_5$ and G_6 is trivial. In the ray class field constructions of function fields with many rational places [9], there is a function field over $\mathbb{F}_8$ with an identical sequence of ramification groups. It has degree 8, as an extension of the rational function field, and genus $g = 14$, for $N = 65$ rational places. Thus, the ratio $N/g = 4.64$. The function field in our example has $N = 33$ and $g = 6$, giving a ratio of $N/g = 5.5$.

6   Generalization of the Hermitian function field

The simplest example of a symmetric function field is the Hermitian function field itself, described below.

Let $F = \mathbb{F}_{q^2}(x)$ and $E = F(y)$ where y satisfies the equation

$$y^q + y = x^{q+1}.$$

Then E is called the Hermitian function field. We have that $g(E) = \frac{q(q-1)}{2}$, and $N(E) = q^3 + 1$, which is the maximum number allowed by the Hasse-Weil bound for this value of genus. Furthermore, the Hermitian function field is the unique maximal function field over $\mathbb{F}_{q^2}$ of genus $g \geq \frac{q(q-1)}{2}$ [4]. The Hermitian function field remains maximal for all values of q. Other symmetric function fields do not exhibit such a uniform performance. For instance, the function fields of Example 4.15 and Example 4.16 attain the the Oesterle bound for $q = 2$, while for higher values of q, they deviate considerably from the Oesterle bound. The other unique feature of the Hermitian function field is the extremely large size of its automorphism group [20].

It has often been implicitly assumed that function field E_n described by Theorem 4.14, called the trace-norm function field, is the generalization of the Hermitian function field for $n \geq 3$. However, we argue below that it is the function field E_2 described by Theorem 4.14 that is more the generalization. It is clear that both coincide for $n = 2$ and in this case, they are just the Hermitian function field. For $n \geq 3$, we must decide which is the more appropriate generalization of the Hermitian function field. We now show the following similarities.

A. Genus

We have already observed that for the $n-1$ families of symmetric extensions $E_i, 2 \leq i \leq n$ described by Theorem 4.14,

$$g(E_2) < g(E_3) \ldots < g(E_n).$$

Thus, among these families E_2 has the lowest genus while the trace-norm function field has the highest.

B. Automorphisms

It is well known [21] that for every δ and τ in $\mathbb{F}_{q^2}$ that satisfy $\tau^q + \tau = \delta^{q+1}$, there is an automorphism σ of the Hermitian function field given by

$$\begin{aligned} \sigma(x) &= x + \tau, \\ \sigma(y) &= y + x\tau^q + \delta. \end{aligned}$$

We can state the general theorem about automorphisms of the symmetric function field $E = F(y)$ where y satisfies (1) for $i = 2$.

Theorem 6.1 *Let* $F = K(x)$ *where* $K = \mathbb{F}_{q^n}$. *Let* $E = F(y)$, *where* y *satisfies the equation*

$$y^{q^{n-1}} + y^{q^{n-2}} + \ldots + y = s_{n,2}(x). \tag{4}$$

Let (δ, τ) *satisfy* $\delta, \tau \in K$ *and*

$$\delta^{q^{n-1}} + \delta^{q^{n-2}} + \ldots + \delta = s_{n,2}(\tau).$$

Let $m = \lfloor \frac{n-1}{2} \rfloor$. *Then there exists an automorphism* σ *of* E *given by*

$$\begin{aligned} \sigma(x) &= x + \tau, \\ \sigma(y) &= y + x\tau^q + x\tau^{q^2} + \ldots + x\tau^{q^{n-1}} + \delta. \end{aligned}$$

The set of these automorphisms keeps F *fixed and forms a subgroup* Γ *of order* q^{2n-1} *of the full automorphism group of the function field* E/K. *Γ acts transitively on the set of finite rational places of* E.

Proof. On expanding $s_{n,2}(x + \tau)$, we observe that there are, apart from all the terms of $s_{n,2}(x)$ and $s_{n,2}(\tau)$, cross terms in x and τ with all possible pairs

31

of exponents $\{q^i, q^j\}$ for x and τ, where $i \neq j$, $0 \leq i,j \leq n-1$. Thus, there are $n(n-1)$ such cross terms, all distinct. On expanding $[\sigma(y)]^{q^{n-1}} + [\sigma(y)]^{q^{n-2}} + \ldots + \sigma(y)$, we get $n(n-1)$ cross terms in x and τ, all distinct, with the same exponent pairs as earlier. □

C. Places of degree two

Let us denote by $N_m(E)$ the number of rational places of degree m in a function field E. Thus, N_m is the number of Galois conjugacy classes of "new" rational points of the curve over the extension of degree m of the original field of definition (*i.e.*, points that belong strictly to the extension, and not to the original field). For the Hermitian function field over $\mathbb{F}_{q^2}$, $N_2 = 0$. This means that there are no "new" rational places over $\mathbb{F}_{q^4}$ – the number of rational points over both the fields is q^3+1. The same phenomenon occurs in each of the other "Deligne-Lusztig" curves, namely the Suzuki and the Ree curves.

Lemma 6.2 *Let the hypotheses be as in Theorem 4.14. Then $N_2(E_i) \neq 0$ only if there exist α, β, such that*

$$\beta^{q^{n-1}} + \beta^{q^{n-2}} + \ldots + \beta = s_{n,i}(\alpha),$$

with $\alpha \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that $s_{n-1,i-1}(\alpha) \in \mathbb{F}_{q^n}$.

Proof. Let $(x,y) = (\alpha, \beta)$ satisfy (1). Then, raising the equation to the qth power and subtracting the original from it, we get

$$\beta^{q^n} - \beta = [s_{n-1,i-1}(\alpha)]^q(\alpha^{q^n} - \alpha).$$

Now raising both sides to the power of q^n, we get that if α and β are elements of $\mathbb{F}_{q^{2n}}$, then

$$\beta - \beta^{q^n} = [s_{n-1,i-1}(\alpha)]^{q^{n+1}}(\alpha - \alpha^{q^n}).$$

Then adding the two equations, we get that either $\alpha = \alpha^{q^n}$ or $[s_{n-1,i-1}(\alpha)]^q = [s_{n-1,i-1}(\alpha)]^{q^{n+1}}$. But since $\alpha \notin \mathbb{F}_{q^n}$, and $\mathbb{F}_{q^n}$ is closed under taking q^{th} powers, this gives us the result. □

EXAMPLE 6.3 *In the case of the Hermitian function field, since $s_{1,1}(x) = x$, Lemma 6.2 precludes any possibility for $N_2 \neq 0$.*

We now need another lemma.

Lemma 6.4 *For $n \neq 3, 4, 6$, There exists no $\alpha \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that $s_{n-1,1}(\alpha) \in \mathbb{F}_{q^n}$.*

Proof. Assume there is such an element α. Then we have that

$$\alpha^{q^{n-2}} + \alpha^{q^{n-3}} + \ldots + \alpha \in \mathbb{F}_{q^n},$$

which gives, on raising to the power of q

$$\alpha^{q^{n-1}} + \alpha^{q^{n-2}} + \ldots + \alpha^q \in \mathbb{F}_{q^n}.$$

Subtracting the first equation from the second, we get

$$\alpha^{q^{n-1}} - \alpha \in \mathbb{F}_{q^n}.$$

This implies that

$$\alpha^{q^{2n-1}} - \alpha^{q^n} = \alpha^{q^{n-1}} - \alpha.$$

Now raising both sides to the power of q^{n-1}, we get

$$\alpha^{q^{n-2}} - \alpha^{q^{2n-1}} = \alpha^{q^{2n-2}} - \alpha^{q^{n-1}}.$$

Adding this equation to the previous one, we get

$$\alpha^{q^{n-2}} - \alpha^{q^n} = \alpha^{q^{2n-2}} - \alpha.$$

This gives us

$$\alpha^{q^n} - \alpha \in \mathbb{F}_{q^{n-2}}.$$

For this to hold, we would need $\mathbb{F}_{q^{n-2}}$ to be a subfield of $\mathbb{F}_{q^{2n}}$, or, $n-2 \mid 2n$. But for $n - 2 > 0$, this happens only for $n = 3, 4$ and 6. $\qquad \square$

Theorem 6.5 *If $n \neq 3, 4$ or 6,*

$$N_2(E_2) = 0.$$

Proof. Follows from Lemma 6.2 and Lemma 6.4. $\qquad \square$

We conclude this paper with an interesting insight into the curves corresponding to symmetric function fields. On any curve, for rational point (α, β) on the curve, the point's conjugate points $(\alpha^{q^i}, \beta^{q^i}), 1 \leq i \leq n - 1$, also lie on the curve. However, in general, points $(\alpha, \beta^{q^i}), 1 \leq i \leq n - 1$, and $(\alpha^{q^i}, \beta), 1 \leq i \leq n - 1$, do not lie on the curve. In the case of a curve corresponding to a symmetric extension of the rational function field, however, these points too lie on the curve. Thus we get many rational points "for free". Similarly, we get many automorphisms also.

7   Conclusion

We have developed a theory that produces infinite families of function fields in which all finite rational places split completely. This theory works over all non-prime finite fields and thus explains, and does away with, the constraints of square cardinality on several existing examples and unifies them under one umbrella. The theory also provides a generalization of the Hermitian function field over non-square finite fields. Further research along the lines of generalizing the notions of symmetry developed in this paper have already been very fruitful leading to several new results ([?, ?]) on the existence and explicit construction of function fields and towers with interesting properties.

Acknowledgements

References

[1] R. A. Beaumont and R. S. Pierce, *The algebraic foundations of mathematics*, Addison-Wesley, Reading, Mass., 1963.

[2] V. Deolalikar, *On splitting places of degree one in extensions of algebraic function fields, towers of function fields meeting asymptotic bounds, and explicit basis constructions for algebraic-geometric codes.*, Ph.D dissertation, Department of Electrical Engineering, University of Southern California, 1999.

[3] M. Fried, "Global construction of general exceptional covers with motivation for applications to encoding," Contemp. Math., **168**, Amer. Math. Soc., Providence, RI, 1994.

[4] R. Fuhrmann and H. Stichtenoth, "On maximal curves," Journal of Number Theory, **67**, 1997, pp. 29-51.

[5] A. Garcia and H. Stichtenoth, "A Tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound," Inventiones Mathematicae, **121**, 1995, pp. 211-222.

[6] A. Garcia and H. Stichtenoth, "On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields," Journal of Number Theory, **61**, No. 2, 1996, pp. 248-273.

[7] A. Garcia and H. Stichtenoth, "Asymptotically good towers of function fields over finite fields," C. R. Acad. Sci. Paris, t. **322**, Série I, 1996, pp. 1067-1070.

[8] V. D. Goppa, "Codes on algebraic curves," Soviet Math. Doklady, **24**, No. 1, 1981, pp. 170-172.

[9] K. Lauter, "Ray class field constructions of curves over finite fields with many rational points," Algorithmic Number Theory, ed. H. Cohen, Lecture Notes in Computer Science, **1122**, Springer, 1996, pp. 187-195.

[10] K. Lauter, "A formula for constructing curves over finite fields with many rational points," Journal of Number Theory, **74**, No. 1, 1999, pp. 56-72.

[11] H. Niederreiter and C.P. Xing, "Cyclotomic function fields, Hilbert Class fields, and global function fields with many rational places," Acta Arithmetica, **79**, No. 1, 1997, pp. 59-76.

[12] A. N. Parshin and I. R. Shafarevich, Eds., *Number Theory II,* Encyclopaedia of Mathematical Sciences, **62**, Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[13] H.-G. Rück and H. Stichtenoth, "A characterization of Hermitian function fields over finite fields," J. Reine Agnew. Math., **457**, 1994, pp. 185-188.

[14] R. Schoof, "Algebraic curves over $\mathbb{F}_2$ with many rational points," Journal of Number Theory, **41**, 1992, pp. 6-14.

[15] R. Schoof, *Algebraic curves and coding theory*, Undergraduate Texts in Math., **336**, Univ. of Trento, 1990.

[16] J.-P. Serre, *Local Fields*, Springer GTM, New York, 1979.

[17] J.-P. Serre, "Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini," C. R. Acad. Sci. Paris Série I Math., **296**, 1983, pp. 397-402.

[18] J.-P. Serre, "Nombres de points des courbes algébriques sur $\mathbb{F}_q$, Sém. Théorie des Nombres 1982-1983, Exp. 22, Univ. de Bordeaux I, Talence, 1983.

[19] J.-P. Serre, *Rational points on curves over finite fields*, Lecture Notes, Harvard University, 1985.

[20] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkrpers von Primzahlcharakteristik. I. Eine Abschtzung der Ordnung der Automorphismengruppe," (German) Arch. Math. (Basel) **24**, 1973, pp. 527-544.

[21] H. Stichtenoth, "A note on Hermitian codes over $GF(q^2)$," IEEE transactions on Information Theory, **34**, No. 5, September 1988, pp. 1345-1348.

[22] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Universitext, Berlin-Heidelberg-New York, 1991.

[23] F. J. Sullivan, "p-torsion in the class group of curves with too many automorphisms," Arch. Math., **26**, 1975, pp. 253-261.

[24] E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

[25] C. P. Xing, "Multiple Kummer extension and the number of prime divisors of degree one in function fields," Journal of Pure and Applied Algebra, **84**, 1993, pp. 85-93.